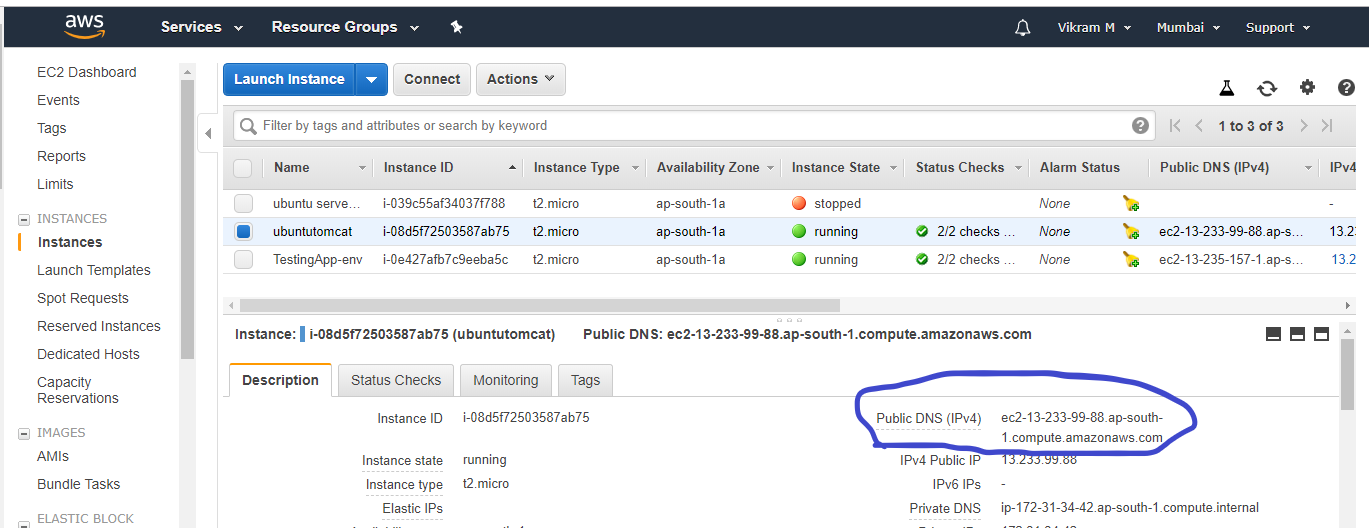
**Setup EC2 instance:**

There are few ways you’ll want to differ from the tutorial:

* We select the “**Amazon Linux AMI 2017.03.1 (HVM), SSH Volume Type**” as **AMI**. The exact versions may change with time.
* We configure the **security groups** as below. This setting allows access to port **80** (**HTTP**) from anywhere, and **SSH** access also.

****

* Go ahead and launch the instance, it will take couple of minutes:

****

**Accessing EC2 instance via SSH using Putty**

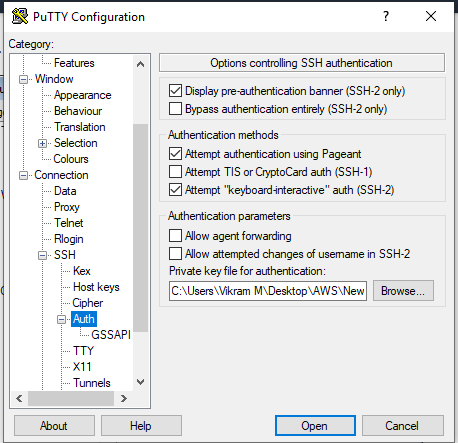
* We need to convert Private Key Using PuTTYgen

**To convert the private key**

1. From the **Start** menu, choose **All Programs**, PuTTY, PuTTYgen.
2. Under **Type of key to generate**, choose **RSA**.
3. Choose **Load**. By default, PuTTYgen displays only files with the extension .ppk. To locate your .pem file, select the option to display files of all types.
4. Select your .pem file for the key pair that you specified when you launched your instance and choose **Open**. Choose **OK**.
5. To save the key in the format that PuTTY can use, choose **Save private key**. PuTTYgen displays a warning about saving the key without a passphrase. Choose **Yes**.
6. Specify the same name for the key that you used for the key pair (for example, my-key-pair). PuTTY automatically adds the .ppk file extension.

**To connect to your instance using PuTTY**

1. Start Putty (from the **Start** menu, choose **All Programs, Putty, Putty**).
2. In the **Category** pane, choose **Session** and complete the following fields:
3. In the **Host Name** box, enter *user\_name*@*public\_dns\_name*. Be sure to specify the appropriate user name for your AMI. For example: For Amazon Linux 2 or the Amazon Linux AMI, the user name is ec2-user.
4. Under Connection type, select SSH
5. Ensure that the port value is 22.
6. In the **Category** pane, expand **Connection**, expand **SSH**, and then choose **Auth**. Complete the following:
7. Choose **Browse**.
8. Select the .ppk file that you generated for your key pair and choose **Open**.
9. (Optional) If you plan to start this session again later, you can save the session information for future use. Under **Category**, choose **Session**, enter a name for the session in **Saved Sessions**, and then choose **Save**.
10. Choose **Open**.
11. If this is the first time you have connected to this instance, PuTTY displays a security alert dialog box that asks whether you trust the host to which you are connecting.



**To install Docker on an Amazon EC2 instance**

1. Launch an instance with the Amazon Linux 2 AMI.
2. Connect to your instance.
3. Update the installed packages and package cache on your instance. **sudo yum update –y**
4. Install the most recent Docker Community Edition package. **sudo amazon-linux-extras install docker**
5. Start the Docker service. **sudo service docker start**
6. Verify that the ec2-user can run Docker commands without sudo. Docker info

**Create a Docker Image**

1. Create a file called Dockerfile. A Dockerfile is a manifest that describes the base image to use for your Docker image and what you want installed and running on it.
2. Build the Docker image from your Dockerfile. **docker build -t nebula .**
3. Run **docker images** to verify that the image was created correctly. **docker images ls**
4. Run the newly built image. The -p 80:80 option maps the exposed port 80 on the container to port 80 on the host system. For more information about **docker run**. **docker run -t -i -p 80:80 nebula**
5. Open a browser and point to the server that is running Docker and hosting your container.
6. If you are using an EC2 instance, this is the **Public DNS** value for the server, which is the same address you use to connect to the instance with SSH. Make sure that the security group for your instance allows inbound traffic on port 80. **docker-machine ip *machine-name***
7. Stop the Docker container by typing **Ctrl + c**.